

EXHIBIT A

Redacted Motion for Class Cert

James M. Wagstaffe (95535)
**ADAMSKI MOROSKI MADDEN
CUMBERLAND & GREEN LLP**
P.O. Box 3835
San Luis Obispo, CA 93403-3835
Tel: 805-543-0990
Fax: 805-543-0980
wagstaffe@ammcglaw.com

*Counsel for Plaintiffs Erica Frasco
and Sarah Wellman*

Christian Levis (*pro hac vice*)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com

*Interim Co-Lead Counsel for Plaintiffs and the
Proposed Class*

Carol C. Villegas (*pro hac vice*)
LABATON KELLER SUCHAROW LLP
140 Broadway
New York, NY 10005
Tel: (212) 907-0700
Fax: (212) 818-0477
cvillegas@labaton.com

*Interim Co-Lead Counsel for
Plaintiffs and the Proposed Class*

Diana J. Zinser (*pro hac vice*)
SPECTOR ROSEMAN & KODROFF, P.C.
2001 Market Street, Suite 3420
Philadelphia, PA 19103
Tel: (215) 496-0300
Fax: (215) 496-6611
dzinser@srkattorneys.com

*Interim Co-Lead Counsel for Plaintiffs and the
Proposed Class*

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

ERICA FRASCO, et al., individually and on
behalf of all others similarly situated,

Plaintiffs,

v.

FLO HEALTH, INC., META PLATFORMS,
INC., GOOGLE, LLC, and FLURRY, INC.,

Defendants.

Case No.: 3:21-cv-00757-JD

**PLAINTIFFS' MOTION FOR CLASS
CERTIFICATION**

Date: November 21, 2024

Time: 10:00 a.m.

Location: Courtroom 11, 19th Floor

Judge: Hon. James Donato

FILED UNDER SEAL

NOTICE OF MOTION

PLEASE TAKE NOTICE that on November 21, 2024 at 10:00 a.m., or another date and time to be determined by the Court, the undersigned will appear before the Honorable James Donato of the United States District Court for the Northern District of California at the San Francisco Courthouse, Courtroom 11, 19th Floor, 450 Golden Gate Avenue, San Francisco, California, 94102, and will move this Court, pursuant to Federal Rule of Civil Procedure 23, for an order certifying the following Proposed Classes:

Under Fed. R. Civ. P. 23(b)(3)		
Class	Representatives	Claims
<u>Nationwide Damages Class:</u> All Flo App users who entered menstruation and/or pregnancy information into the Flo Health App between November 1, 2016 and February 28, 2019, inclusive.	Plaintiffs Erica Frasco, Sarah Wellman, Jennifer Chen, Tesha Gamino, and Autumn Meigs	<u>Against Defendant Flo Health, Inc.:</u> (1) violation of the California Confidentiality of Medical Information Act ("CMIA"); (2) breach of contract (or in the alternative breach of an implied contract); (3) common law invasion of privacy (intrusion upon seclusion); and (4) violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA") <u>Against Defendants Meta, Inc., Google, Inc., Flurry, Inc.:</u> (1) violation of CDAFA; and (2) aiding and abetting a common law invasion of privacy violation (intrusion upon seclusion)
<u>California Subclass:</u> All Flo App users in California who entered menstruation and/or pregnancy information into the Flo Health App while residing in California between November 1, 2016 and February 28, 2019, inclusive.	Plaintiffs Sarah Wellman, Jennifer Chen, and Tesha Gamino	All claims asserted by the Nationwide Class, plus: <u>Against Defendant Flo Health, Inc.:</u> invasion of privacy in violation of Art. 1, Sec. 1 of the California Constitution <u>Against Defendants Meta, Inc., Google, Inc., Flurry, Inc.:</u> violation of the California Invasion of Privacy Act ("CIPA")
Under Fed. R. Civ. P. 23(b)(2)		
Class	Representatives	Claims
<u>Injunctive Relief Class:</u> All Flo App users who entered menstruation and/or	Plaintiffs Erica Frasco, Sarah Wellman, Jennifer Chen,	<u>Against All Defendants:</u> for injunctive relief in connection

pregnancy information into the Flo Health App between November 1, 2016 and February 28, 2019, inclusive.	Tesha Gamino, and Autumn Meigs	with their CDAFA, and common law invasion of privacy claims.
<u>California Subclass:</u> All Flo App users in California who entered menstruation and/or pregnancy information into the Flo Health App while residing in California between November 1, 2016 and February 28, 2019, inclusive.	Plaintiffs Sarah Wellman, Jennifer Chen, and Tesha Gamino	<u>Against Defendants Meta, Inc., Google, Inc., Flurry, Inc;</u> in connection with their CIPA claims

Plaintiffs seek the appointment of these Plaintiffs as Class Representatives. Plaintiffs also seek appointment of Carol Villegas (Labaton Keller Sucharow), Christian Levis (Lowey Dannenberg), and Diana Zinser (Spector Roseman & Kodroff) as Class Counsel.

The Motion is based upon this Notice, the Memorandum of Law, the declaration of Carol C. Villegas (hereinafter “Villegas Decl.”), the Plaintiffs’ declarations, all exhibits to such documents, any papers filed in reply, and any argument as may be presented at the hearing.

STATEMENT OF ISSUES TO BE DECIDED

Whether Plaintiffs have shown by a preponderance of the evidence that: (1) the Proposed Classes satisfy Rule 23(a)’s requirements; (2) the Nationwide Damages Class and California Subclass satisfy Rule 23(b)(3)’s predominance and superiority requirements; (3) whether the Injunctive Relief Class meets Rule 23(b)(2)’s requirements.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	STATEMENT OF FACTS	2
III.	LEGAL STANDARD	12
IV.	ARGUMENT	12
A.	The Proposed Classes Meet Rule 23(a)'s Requirements.	12
B.	Common Questions of Law and Fact Predominate Over Individual Issues.	13
C.	The Claims of the Classes Satisfy Predominance	14
1.	California Law Applies to Each of the Classes' Claims	14
2.	Claims Against Flo.....	14
a.	CMIA	14
b.	Breach of Contract	16
c.	Intrusion Upon Seclusion	16
d.	CDAFA	18
3.	Claims Against Ad Defendants.....	19
a.	CDAFA	19
b.	Aiding and Abetting Intrusion Upon Seclusion	19
D.	The California Subclass	20
1.	Invasion of Privacy Under the California Constitution Against Flo.....	20
2.	Violation of CIPA Against the Ad Defendants.....	20
E.	Common Issues Predominate Regarding the Relief Plaintiffs Seek	21
1.	Statutory Damages	21
2.	Punitive Damages.....	22
3.	Nominal Damages.....	23
4.	Disgorgement	23
F.	A Class Action Is the Superior Method of Adjudicating This Dispute.....	24
G.	The Proposed Injunction Class Meets Rule 23(b)(2)'s Requirements.....	24
a.	The Court Should Appoint Class Counsel.	25

V.	CONCLUSION	25
----	------------------	----

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Amgen Inc. v. Conn. Ret. Plans and Tr. Funds</i> , 568 U.S. 455 (2013)	12
<i>Briseno v. ConAgra Foods, Inc.</i> , 844 F.3d 1121 (9th Cir. 2017)	24
<i>Brown v. Google LLC</i> , 525 F. Supp. 3d 1049 (N.D. Cal. 2021)	16, 17
<i>Brown v. Google, LLC</i> , No. 20-cv-3664-YGR, 2022 WL 17961497 (N.D. Cal. Dec. 12, 2022)	21
<i>Calhoun v. Google LLC</i> , 526 F. Supp. 3d 605 (N.D. Cal. 2021)	17
<i>Coulter v. Bank of Am.</i> , 28 Cal. App. 4th 923 (1994)	22
<i>CTI III, LLC v. Devine</i> , No. 2:21-CV-02184-JAM-DB, 2022 WL 1693508 (E.D. Cal. May 26, 2022)	19
<i>Doe v. Regents of Univ. of Cal.</i> , No. 23-CV-00598-WHO, 2023 WL 3316766 (N.D. Cal. May 8, 2023)	17
<i>Dulberg v. Uber Techs., Inc.</i> , No. C 17-00850 WHA, 2018 WL 932761 (N.D. Cal. Feb. 16, 2018)	16
<i>DZ Reserve v. Meta Platforms, Inc.</i> , No. 3:18-cv-04978-JD, 2022 WL 912890 (N.D. Cal. Mar. 29, 2022)	23, 24
<i>Ellis v. Costco Corp.</i> , 285 F.R.D. 492 (N.D. Cal. 2012)	22
<i>In re Facebook, Inc. Internet Tracking</i> , 956 F.3d 589 (9th Cir. 2020)	16, 17, 20, 23
<i>In the Matter of Flo Health, Inc.</i> , FTC No. C-4747, Decision and Order (June 17, 2021)	12
<i>Francies v. Kapla</i> , 127 Cal. App. 4th 1381 (Cal. Ct. App. 2005)	22
<i>In re Google Inc. Gmail Litig.</i> , No. 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013)	20
<i>Greenley v. Kochava, Inc.</i> , No. 22-CV-01327-BAS-AHG, 2023 WL 4833466 (S.D. Cal. July 27, 2023)	18, 20

1	<i>Jackson v. First Nat'l Bank of Omaha,</i>	
2	No. CV 20-1295 DSF (JCX), 2022 WL 423440 (C.D. Cal. Jan. 18, 2022).....	22
3	<i>Just Film, Inc. v. Buono,</i>	
4	847 F.3d 1108 (9th Cir. 2017).....	21, 24
5	<i>In re JUUL Labs, Inc., Mktg. Sales Pracs. & Prod. Liab. Litig.,</i>	
6	609 F. Supp. 3d 942 (N.D. Cal. 2022)	12
7	<i>Kellman v. Spokeo, Inc.,</i>	
8	No. 21-CV-08976-WHO, 2024 WL 2788418 (N.D. Cal. May 29, 2024)	22
9	<i>Kumandan v. Google, LLC,</i>	
10	No. 19-cv-04286-BLF, 2023 WL 8587625 (N.D. Cal. Dec. 11, 2023)	16
11	<i>Liu v. SEC,</i>	
12	140 S.Ct. 1936 (2020)	23
13	<i>McCrary v. Elations Co., LLC,</i>	
14	No. EDCV 13-00242 JGB OP, 2014 WL 1779243 (C.D. Cal. Jan. 13, 2014)	20
15	<i>Meister v. Mensinger,</i>	
16	230 Cal. App. 4th 381 (Cal. Ct. App. 2014)	23
17	<i>In re Meta Pixel Healthcare Litig.,</i>	
18	No. 22-cv-03580-WHO, 2022 WL 7869218 (N.D. Cal. Dec. 22, 2022)	20
19	<i>Nitsch v. Dreamworks Animation SKG Inc.,</i>	
20	315 F.R.D. 270 (N.D. Cal. 2016)	14
21	<i>NovelPoster v. Javitch Canfield Grp.,</i>	
22	140 F. Supp. 3d 954 (N.D. Cal. 2014)	18-19
23	<i>Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC,</i>	
24	31 F.4th 651 (9th Cir. 2022).....	12, 13, 14
25	<i>Opperman v. Path, Inc.,</i>	
26	84 F. Supp. 3d 962 (N.D. Cal. 2015)	19
27	<i>Opperman v. Path, Inc.,</i>	
28	No. 13-cv-0453-JST, 2016 WL 3844326 (N.D. Cal. July 15, 2016)	17, 19, 22, 23
	<i>Owino v. CoreCivic, Inc.,</i>	
	60 F.4th 437 (9th Cir. 2022).....	21
	<i>Parra v. Bashas', Inc.,</i>	
	536 F.3d 975 (9th Cir. 2008).....	12
	<i>In re Premera Blue Cross Customer Data Sec. Breach Litig.,</i>	
	No. 3:15-MD-2633-SI, 2019 WL 3410382 (D. Or. July 29, 2019)	15
	<i>Pulaski & Middleman,</i>	
	802 F.3d 979 (9th Cir. 2015).....	21

1	<i>In re Qualcomm Antitrust Litig.</i> ,	
2	292 F. Supp. 3d 948 (N.D. Cal. 2017)	14
3	<i>Rodriguez v. Google LLC</i> ,	
4	No. 20-CV-04688-RS, 2024 WL 38302 (N.D. Cal. Jan. 3, 2024)	13, 16, 17, 18
5	<i>Roley v. Google LLC</i> ,	
6	Case No. 18-v-07537-BLF, 2020 WL 8675968 (N.D. Cal. July 20, 2020)	16
7	<i>In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.</i> ,	
8	613 F. Supp. 3d 1284 (S.D. Cal. 2020)	23
9	<i>Stasi v. Inmediata Health Grp. Corp.</i> ,	
10	501 F. Supp. 3d 898 (S.D. Cal. 2020)	23
11	<i>In re Static Random Access Memory (SRAM) Antitrust Litig.</i> ,	
12	264 F.R.D. 603 (N.D. Cal. 2009)	12
13	<i>Steven Ades & Hart Woolery v. Omni Hotels Mgmt. Corp.</i> ,	
14	No. 2:13-CV-02468-CAS, 2014 WL 4627271 (C.D. Cal. Sept. 8, 2014)	21-22
15	<i>Ticketmaster L.L.C. v. Prestige Ent. W., Inc.</i> ,	
16	315 F. Supp. 3d 1147 (C.D. Cal. 2018)	18
17	<i>Tyson Foods, Inc. v. Bouaphakeo</i> ,	
18	577 U.S. 442 (2016)	13
19	<i>Varnado v. Midland Funding LLC</i> ,	
20	43 F. Supp. 3d 985 (N.D. Cal. 2014)	22
21	<i>Vigil v. Muir Med. Grp. IPA, Inc.</i> ,	
22	84 Cal. App. 5th 197 (Cal. Ct. App. 2022)	14-15
23	<i>Ward v. United Airlines, Inc.</i> ,	
24	9 Cal. 5th 732 (2020)	14
25	<i>Wolin v. Jaguar Land Rover N. Am., LLC</i> ,	
26	617 F.3d 1168 (9th Cir. 2010)	13
27	<i>In re Yahoo Mail Litig.</i> ,	
28	308 F.R.D. 577 (N.D. Cal. 2015)	13, 24
	Statutes & Rules	
	Cal. Civ. Code § 56.05(i)	15
	Cal. Civ. Code § 56.10	14, 15
	Cal. Civ. Code § 3294	22
	California Invasion of Privacy Act	<i>passim</i>
	Cal. Penal Code § 502	18, 19
	Cal. Penal Code § 637.2(a)	21

1	California Confidentiality of Medical Information Act.....	<i>passim</i>
2	California Constitution.....	20
3	Comprehensive Computer Data Access and Fraud Act.....	<i>passim</i>
4	Fed. R. Civ. P. 23	<i>passim</i>

1 **I. INTRODUCTION**

2 This case concerns the systematic collection, disclosure, and commercial exploitation of
3 millions of women’s reproductive health information by Defendant Flo Health, Inc. (“Flo”), maker
4 of the Flo Period & Ovulation Tracker mobile app (the “Flo App”), and three of the largest advertising
5 and analytics companies: Defendants Google, LLC, Meta Platforms, Inc., and Flurry, Inc.
6 (collectively, the Ad Defendants or “ADs”).

7 Marketed as a way for women to take control of their health, the Flo App promised to be a
8 secure platform for privately tracking the intimate details of one’s reproductive health. In reality, it
9 allowed the Ad Defendants to intercept billions of data points about the inner workings of women’s
10 bodies. Shockingly granular details, including whether an individual was pregnant or ovulating, and
11 the dates and duration of their periods, were transmitted from the Flo App to each Ad Defendant
12 through specialized Software Development Kits (“SDKs”), that Flo incorporated into its app between
13 November 1, 2016 and February 28, 2019 (the “Class Period”).

14 Flo *intended* this health information to be intercepted as it specifically programmed the app
15 to execute Ad Defendants’ SDK code when users logged data about their period or pregnancy. Flo
16 used this information to acquire new app users by marketing to them based on their reproductive goals
17 (e.g., getting pregnant). Ad Defendants separately used the data they intercepted for their own
18 commercial purposes. Meta used health information it received from the Flo App for research and
19 development, as well as to optimize the ads it displayed to Facebook users. Google utilized the data
20 it received through its SDKs within its own advertising systems. And Flurry, which Yahoo acquired
21 specifically to boost its mobile ad revenue, provided its parent company with a data feed containing
22 Flo App’s users’ health information.

23 Plaintiffs, like millions of other women who used the Flo App, were injured when the health
24 information they privately entered was intercepted and used without their consent. Each of their
25 damages claims, like those of the Proposed Class’s members, presents common questions that can be
26 answered through common evidence, including documents and data relating to Defendants’ collection
27 and use of health information from the Flo App, and failure to obtain consent for such conduct.
28 Injunctive relief is also necessary to stop the Ad Defendants’ ongoing misuse of Class members’

health information, as there is no indication this data has been removed from Defendants’ machine learning algorithms or processes. Likewise, Flo should be enjoined from continuing to violate Class members’ privacy by disclosing health information without first obtaining affirmative consent in compliance with applicable laws. The Court should grant Plaintiffs’ motion in its entirety.

II. STATEMENT OF FACTS

The Flo App. With more than [REDACTED] users in the U.S., and millions in California, the Flo App is the most popular period-tracking app in the United States. *See* Ex. 1; Ex. 2.^{1 2} Flo claims the app allows users to take “full control of [their] health” by tracking their menstrual cycle, predicting ovulation, helping users get pregnant, tracking their baby development, and assisting with postpartum recovery. Ex. 3; Ex. 4 at ‘091.

All Flo App users must complete an onboarding survey the first time they use the app. Ex. 5 ¶¶40-41; Ex. 6. The onboarding survey in effect during the Class Period required all Flo App users, including Plaintiffs, to enter their age and select a “goal” from three options: (1) track my cycle (2) get pregnant; or (3) track pregnancy. Ex. 6 at ‘805. Users are then prompted to enter the date and length of their last period. *Id.* If the user is pregnant, the survey asks how many weeks she is into her pregnancy. Ex. 7 at ‘891. Once the onboarding survey is complete, Flo users log daily “symptoms” and monthly menstrual cycles to receive “health insight[s]” and “predictions.” Ex. 6 at ‘812-29.

Software Development Kits (“SDKs”) in the Flo App. Over the Class Period, Flo released various versions of its Flo App for Android and iOS devices. Ex. 5 ¶¶43, 48. Each of these versions of the Flo App incorporated pre-built libraries of code called SDKs developed by the Ad Defendants. *See* Ex. 8; Ex. 5 ¶¶51-52. The Ad Defendants designed their SDKs specifically to collect data about app users’ activity. Ex. 9 ¶¶5-6; *see, e.g.*, Ex. 10 at ‘460 (“The Flurry iOS Analytics Agent allows you to track the usage and behavior of your iOS application on users’ phones for viewing in the Flurry Analytics system.”); Ex. 11 at ‘788 (“Google Analytics collects usage and behavior data for your app.”); Ex. 12 at ‘939 (Meta’s SDK allows an app developer to “better understand your app users, . .

¹ All exhibits cited in this motion are attached to the Villegas Decl., attached hereto.

² Flo possesses the actual number of California users in its own records. Indeed, Flo maintains location data for each user, including Plaintiffs, as described in Section II. pp. 7-8. *See also* Declarations of Jennifer Chen, Erica Frasco, Tesha Gamino, Autumn Meigs, and Sarah Wellman (“Plaintiffs’ Declarations”), attached hereto.

1 . [and] measure and optimize app events taking place after the install”).

2 The Ad Defendants’ SDKs intercept and transmit user’s communications with Flo by
3 capturing a users’ in-app interactions, known as app “events.” *See* Ex. 5 ¶¶54, 60-68. Each Ad
4 Defendants’ SDK pre-define certain “Standard Events” to reflect actions common to all apps (*e.g.*,
5 closing the app). They also allow developers to create “Custom Events” relevant to their specific app.
6 Developers choose the user action that will trigger the transmission of a Custom Event (such as
7 clicking a particular button) and can name them accordingly. *See* Ex. 13 at ‘973 (explaining
8 “automatically logged” events” and “custom events”); Ex. 14 at ‘646 (explaining developer can create
9 “up to 500 different” events); Ex. 15 at ‘102 (“You can use custom events to track specific actions
10 users take within your app[.]”); Ex. 16 at ‘154; Ex. 17 at 107:11-13 (“Q: And Flo is the one who
11 defines [custom app events], correct? A: Flo would have been the one to have defined [custom app
12 events].”). Developers can also include “parameters” or “values” in their Custom Events that provide
13 even more detail about the activity the user has taken. *See* Ex. 5 ¶¶69-70, 101; Ex. 18 at ‘019; Ex. 19
14 at ‘046; Ex. 14 at ‘646 (describing “parameter” and “value”); Ex. 20 at 46:6-19 (“Q: So I just want to
15 confirm, the parameter would have been written by Flo Health; is that correct? A: Yes.”).

16 Flo’s Custom Events Disclosed Health Information. The Custom Event data Ad Defendants
17 intercepted from Flo App users reflected these individuals’ communications with Flo regarding their
18 reproductive health. Ex. 5 ¶¶3-5, 69-72. Figure 1 below identifies Custom Events that Flo created in
19 its onboarding that conveyed reproductive health information to the Ad Defendants. *Id.*; Ex. 21 at
20 ‘738 (Flo “sent data back to Google” via these SDKs’ “unique identifiers for each Flo App user, along
21 with Custom Events whose titles conveyed Flo app users’ health information,” including events listed
22 in Figure 1); Ex. 22 at ‘380 (Meta received Flo Custom Events showing “whether on a given day
23 she has her period, is in ovulation, has a delayed period or is pregnant.”).

24 *Figure 1* indicates which Ad Defendant (with an “M” for Meta, “G” for Google, and “F” for
25 Flurry) received each of these events.

FIGURE 1

Custom Event	Corresponding App Action
R_CHOOSE_GOAL	The Flo App User selected a “goal” during the Flo Onboarding Survey (e.g., intention to become pregnant) (received by M, G, F).
R_SELECT_LAST_PERIOD_DATE	The Flo App User selected the date of their last period during the Flo Onboarding Survey (received by M, G, F).
R_SELECT_CYCLE_LENGTH	The Flo App User selected the length of their last cycle during the Flo Onboarding Survey (received by M, G, F).
R_SELECT_PERIOD_LENGTH	The Flo App User selected the length of their last period during the Flo Onboarding Survey (received by M, G, F).
R_AGE_CHOSEN_PERIODS	The Flo App User selected they want to track their period and entered their age during the Flo Onboarding Survey (received by M, G, F).
R_AGE_CHOSEN_PREGNANCY	The Flo App User selected they are pregnant, know the week of their pregnancy, and entered their age during the Flo Onboarding Survey (received by M, G, F).
R_AGE_CHOSEN_PREGNANCY_METHOD	The Flo App User selected they are pregnant, they do not know the week of their pregnancy, and entered their age during the Flo Onboarding Survey (received by M, G, F).
R_PREGNANCY_METHOD	The Flo App User selected they were pregnant and chose “other method” to determine their pregnancy term during the Flo Onboarding Survey (received by M, G, F).
R_PREGNANCY_METHOD_DATE	The Flo App User selected they were pregnant and entered the “date for the selected pregnancy” during the Flo Onboarding Survey (received by M, G, F).
R_PREGNANCY_WEEK_CHOSEN	The Flo App user selected they were pregnant and “chose pregnancy week” during the Flo Onboarding Survey (received by M, G, F).
R_PREGNANCY_WEEK_CHOSEN_UNKNOWN	The Flo App user selected they were pregnant and answered “I don’t know” to the question of what pregnancy week they are in during the Flo Onboarding Survey (received by M, G, F).
SESSION_CYCLE_DAY ³	The Flo App predicted the user’s calculated cycle based on the Flo App user’s responses during the onboarding survey. The event parameter CYCLE_DAY relays the number of days they were in their cycle and the parameter CYCLE_DAY_TYPE relays where the user is in their cycle (e.g., ovulating, period, etc.). (received by G, F).

The Ad Defendants’ SDKs contemporaneously intercepted these communications with the Flo App, transmitting the corresponding Custom Event (with parameters) to their servers each time a user took one of the actions in the last column. Ex. 9 ¶¶6-8 (confirming events above were transmitted); Ex. 7 (Flo providing list of transmitted events to FTC); Ex. 23 at ‘147 (Meta “received app events, both Custom and Standard, from Flo Health from *at least* December 9, 2017, through at

³ Meta, Google, and Flurry also received the event “SESSION_CYCLE_DAY_FIRST_LAUNCH,” which was also accompanied by the parameters CYCLE_DAY and CYCLE_DAY_TYPE. *See* Ex. 5 ¶¶60, 69, 81, 94, 103.

1 least December 4, 2019.”). Indeed, Google received each of the Custom Events listed in Figure 1
 2 [REDACTED] of times. *See* Ex. 24 at page 1 of Exhibit C to Second Supp. Resp. to Rog. No. 8 (identifying
 3 Custom Event R_CHOOSE_GOAL received more than [REDACTED] [REDACTED] times and
 4 SESSION_CYCLE_DAY received more than [REDACTED] times). Flurry’s internal “change logs,”
 5 along with a copy of the data it received, likewise confirm that it received each of the Custom Events
 6 listed in Figure 1 through its SDK during the Class Period. Ex. 25 (Flurry’s iOS change logs); Ex. 26
 7 (Flurry’s Android change logs). Meta’s documents do the same. Ex. 27 (identifying Custom Events
 8 in Figure 1 that Facebook received through its SDK); Ex. 23 at ‘147. The parameters transmitted with
 9 these events reveal the user’s selection and convey even more health information than apparent from
 10 the Custom Events’ name. For example, the parameters for R_CHOOSE_GOAL are transmitted with
 11 a parameter revealing the users’ goal selection, *e.g.*, “track_cycle” or “get_pregnant.” Ex. 5 ¶60.

12 This information was so valuable that Flo sold access to the data the Ad Defendants
 13 intercepted to *other third parties*, like Procter & Gamble and Bayer, that wanted to target women
 14 based on their pregnancy status or menstrual cycle. *See* Ex. 28 (email titled “Re: Events for Google
 15 Analytics” explaining that certain “events are needed for [Flo’s] contract with P&G” in the “Google
 16 Analytics feed”); Ex. 29 (same); Ex. 30 (same); Ex. 31 (revenue from P&G and Bayer).⁴

17 Identifying Information Sent With Custom Events. These Custom Events were accompanied
 18 by unique “Advertising IDs” (“AD IDs”)—a type of persistent identifier—corresponding to each Flo
 19 App user. *See* Ex. 32, Resp. to Rog. No. 3 at 38-39; Ex. 33 at ‘904; Ex. 34 at ‘932; Ex. 35 at ‘742 (Flo
 20 “sent back” “unique identifiers” to Google through its SDKs); Ex. 36 at ‘923 (“the SDK collects
 21 personal information (Device Ids), so the only way to not send us personal information is to not
 22 initialize Flurry.”); Ex. 37 at ‘433 (Flo acknowledging that “3rd party analytical systems (e.g. Google
 23 Analytics, Flurry, etc.)” received “personal identifiers...(e.g. IDFA, IP address, advertiser ID, etc)”).

24 AD IDs are considered “personal information” under HIPAA, GDPR, GLBA, CCPA, and
 25 COPPA because they can identify an individual. Ex. 5 ¶27; *see also* Ex. 20 at 60:2-6 (“Q: What is

26 ⁴ Once Apple threatened to pull the Flo App from the App store for sharing data through the Ad
 27 Defendants’ SDKs, Flo stopped giving Bayer access to event data through its Google account and,
 28 instead, provided access directly to its own internal analytics servers. Ex. 37 at ‘429 (Flo employee
 explaining to Bayer they will need to “pull[] all SDK integration” and, instead, engage in “data
 sharing with Bayer . . . directly, rather than via a 3rd party analytics platform”).

your understanding of what an advertising device identifier is? A: It's a unique identifier for a particular device. That can be used to – for identity matching purpose in – in ads.”). Ad Defendants used AD IDs received with Custom Event data to “match” the events to specific individuals. *See* Ex. 5 ¶¶28-39; *see also* Ex. 38, Resp. to Rog 1 at 10-11 (“Apps Device Identifiers” such as “Android Advertiser ID or an Apple ID for Advertisers,” were sent from the Flo App to Meta “for matching purposes”); Ex. 86 at 20.⁵ This was not the only identifying information the Ad Defendants received. Meta also received user emails, full names, phone numbers, dates of birth, and location data with Custom Events so that it could associate that data with an individual’s Facebook account. *See* Ex. 38, Resp. to Rog 1 at 10-11; *see also* Ex. 39 at ‘148; Ex. 40 at ‘151; Ex. 20 at 172:9-14 (confirming “Meta was performing identity matching on the Flo App event data that it received”). Google received AD IDs and other unique user IDs. Ex. 41 at ‘872. Google automatically ties these “User ID[s]” to data already in its systems to identify users, with “no set of protections . . . in place to make that go away.” Ex. 42 at ‘971; Ex. 43 (explaining that UserID is mapped to an ID on Google’s servers and stored with AD IDs); Ex. 122 at ‘497 (confirming Google links these IDs to “demographics and interests information associated with user’s app activity”). And Flurry collected persistent, hardware-linked identifiers that allowed it to associate data with a specific user too. *See* Ex. 44 at 498:5-11 (“Flurry analytics data gets combined and then linked across these other data sets using the Flurry ID or other identifiers that then allows Flurry to track users across devices and then identify them individually”).

Plaintiffs’ Data Disclosed by Flo and Transmitted to ADs. All Flo App users—including Plaintiffs—are required to select a “goal” during the onboarding survey, triggering the Custom Event R_CHOOSSE_GOAL, before they can track their menstrual cycle. *See* Ex. 6 at ‘805; Ex. 7 at ‘891. Because Plaintiffs input *at least* their menstrual cycle information into the Flo App,⁶ they *must have* each selected a “goal,” triggering the Ad Defendants’ interception of this Custom Event. Additionally, Plaintiffs would trigger (and the Ad Defendants would receive) at least the Custom Events

⁵ Google’s use of identifiers to track unique individuals are described more thoroughly in Plaintiffs’ Opposition to Google’s Motion for Summary Judgement. *See* ECF No. 351-3 at 17.

⁶ Ex. 45 at 86:15-17 & Ex. 46 at 12 (confirming Plaintiff Meigs input cycles); Ex. 47 at 87:10-19 & Ex. 48 at 12 (same for Plaintiff Frasco); Ex. 49 at 123:17-24 & Ex. 50 at 11 (same for Plaintiff Chen); Ex. 51 at 103:6-9 & Ex. 52 at 11 (same for Plaintiff Wellman); Ex. 53 at 135:23-136:1 & Ex. 54 at 12 (same for Plaintiff Gamino).

1 CYCLE_DAY and CYCLE_DAY_TYPE when they entered their menstrual cycle information. *See*
 2 Ex. 5 ¶¶69, 101; Ex. 24 at page 1 of Exhibit C to Second Supp. Resp. to Rog. No. 8.

3 Plaintiffs' testimony about tracking their cycle is confirmed by Flo's own data. Flo produced
 4 data associated with Plaintiffs' accounts reflecting menstrual cycle information they entered in the
 5 Flo App during the Class Period. *See* Ex. 55 at '071-84 (Plaintiff Chen); Ex. 56 at '295-307 (Plaintiff
 6 Frasco); Ex. 57 at '110-20 (Plaintiff Gamino); Ex. 58 at '381-85 (Plaintiff Meigs); Ex. 59 at '102-03
 7 (Plaintiff Wellman). Figure 2 illustrates how a portion of menstrual data Plaintiff Frasco entered
 8 appears:

9 **FIGURE 2**



17 Flo maintains nearly identical records for each Plaintiff, and likely all Class members.
 18 Additionally, Flo maintains users' names, emails, user IDs, installation IDs, device IDs, IP addresses
 19 IDFAs, Android Ads IDs, IDFAs, as well as location information reflecting the user's city and state.
 20 *See, e.g.*, Ex. 60; Ex. 61; Ex. 62; Ex. 63; Ex. 64; Ex. 65; Ex. 66; *see also* Plaintiffs' Declarations.

21 The Ad Defendants did nothing to prevent their receipt of this health information. *See* Ex. 67
 22 at 296:3-7 ("Q: So there's no system that would stop it [Flurry via SDK] from receiving health
 23 information? A: There's no system to know that it's health data."); Ex. 20 at 244:12-16 ("And there
 24 was nothing within the SDK code that would prevent that information from being transferred to Meta?
 25 . . . A: No."); Ex. 68 at 47:6-11 ("Technically speaking, as long as the string that is passed in fits
 26 within the length limits and character constraints, the system would allow an app developer to up --
 27 to send such an event [as "cancer status"]."). Despite knowing that sensitive data could be transmitted
 28

1 through the Facebook SDK it was not until December 2019 that Meta—and only Meta—attempted
 2 to develop an “integrity system” that could identify and block health information. *See* Ex. 69 (dated
 3 May 4, 2018) (acknowledging “custom data fields” can “inadvertently (or intentionally) send
 4 sensitive information” including “health info,” presenting “PR issues.”); Ex. 70 at ‘101 (dated March
 5 29, 2018) (asking if there are “concerns on crawling sensitive user data in SDK.”); Ex. 20 at 154:1-
 6 11 (“Before December of 2019, Meta did not do anything to prevent the ingestion of potentially
 7 health-related information received in the form of custom app events through the Facebook SDK; is
 8 that correct?. . . A: That’s right. At -- before that, our integrity system was focused on PI and credit
 9 card information and other -- other information listed in the previous paragraph.”) There is no
 10 evidence Google or Flurry ever did the same.⁷

11 Defendants Used the Custom Events for Their Own Purposes. Flo used Ad Defendants to
 12 generate “actionable insight[s]” from this data to monetize its app. *See* Ex. 19 at ‘046, ‘050 (logging
 13 event data allows app developers to gain “actionable insight[s]” and “monetize better”); Ex. 71, Resp.
 14 to Rog. No. 1 at 6 (explaining Flo’s use of the Flurry SDK allowed Flo to query the data for analytics);
 15 Ex. 38, Resp. to Rog. No. 1 at 12 (acknowledging the purpose of sending event data was so Meta can
 16 perform analytics “regarding the actions users took within the Flo App.”); Ex. 24, Third Supp. Resp.
 17 to Rog. No. 1 at 19 (Flo used Google’s SDKs to collect event data and generate analytics for its
 18 projects “flo-smart-period-tracker” and “flo-health.”). This included leveraging users’ health data.
 19 When Flo sought to replace Flurry’s SDK with a new analytics provider in 2018, one of its
 20 requirements was to profile users based on their “current goal” and pregnancy status—two Custom
 21 Events from the onboarding survey—in addition to other health data. Ex. 72 (listing an “Amplitude
 22 Integration Requirement[]” to create “User Profile[s]” based on the user’s “current goal,” “pregnant
 23 or not,” whether there were “successful birth[s],” whether there were “miscarriages,” “[a]ge,”
 24 “[c]ounty,” “[h]ealth [p]rofile,” “[c]ontraception,” and more).

25 Flo spent heavily on advertising with the Ad Defendants during the Class Period as it sought
 26 to grow its user base. *See, e.g.,* Ex. 75 at ‘270 (Flo spent [REDACTED] on Facebook Ads and [REDACTED]

27 ⁷ While Google moved for summary judgment claiming that it had “features” that limited its ability
 28 to use data it received from the Flo App, this has been categorically debunked. *See* ECF No. 351-3.

1 on Google Adwords in the single month of January 2020, which led to [REDACTED] and [REDACTED] new subscriptions,
2 respectively); Ex. 76 at ‘650-51 (noting in Q1 2021 Flo reached “an important milestone of [REDACTED]
3 of paying subscribers and a new record in revenue ([REDACTED] in MoM)” and considering “new UA
4 strategy” as one of the main driving factors); Ex. 77 at ‘806, ‘809 (Flo’s financials showing
5 subscription revenue of over [REDACTED] in 2019 with advertising expenses equaling less than half
6 that at [REDACTED] Ex. 38, Resp. to Rog. No. 9 at 20 (“During the Relevant Time Period, Meta
7 received [REDACTED] in revenue in connection with advertising that Flo Health conducted . . . based
8 on App Events sent to Meta by the Flo App.”).

9 Google and Meta collaborated with Flo on health-based advertising campaigns to target
10 women based on their reproductive goals. *See, e.g.*, Ex. 73 at ‘510 (explaining Flo’s Google “Ad
11 groups” and “All of [its] audience[s]” are split by the users’ “goal” e.g., track period, pregnant, etc.);
12 Ex. 74 at ‘855-56 (Google acknowledging Flo’s plan to target “women who are planning to get
13 pregnant” and “research about the behavior of pregnant women online”); Ex. 123 (showing Flo’s
14 “Google Ads remarketing lists,” including targeting “get[]pregnant” users and, another one, a
15 “period[]tracker” group); Ex. 78 at ‘317 (listing Google employees who would assist Flo with user
16 acquisition, marketing activities, measurement, and attribution); Ex. 79 (Google presentation to Flo
17 regarding “monetization strategy”); Ex. 80 at ‘232 (providing a “dedicated Account Manager”); Ex.
18 81 at ‘058 (Meta and Flo discussing application of Meta’s algorithm for targeting “pregnant” and
19 “period tracking” app users).

20 These ads, and the health data associated with them, were so valuable that the Ad Defendants
21 violated their own purported advertising policies. Google helped Flo target pregnant women with ads,
22 even though Flo supposedly “prohibited” from advertising to them “directly.” Ex. 82. Internally,
23 Google employees sought to categorize the Flo App as “not sensitive” enough to circumvent certain
24 restrictions on advertisers’ use of health data Google developed after the Class Period. Ex. 83 at ‘738;
25 Ex. 124 at ‘269-70 (feature preventing advertisers from creating remarketing lists for sensitive apps
26 was “pending” as of March 2020). Meta, likewise, provided Flo a dedicated account manager who
27 helped Flo target pregnant women and those tracking their period based on their goals. *See* Ex. 125;
28 *see also* Ex. 126; Ex. 111 (discussing solutions to continue data sharing and avoid “issues for

1 journalists”). This occurred even *after* the *Wall Street Journal* exposed Flo’s illicit use of women’s
 2 health data and sharing with Meta. *See id.*

3 Ad Defendants each took advantage of Custom Event data from Flo for their own commercial
 4 purposes. Meta used Flo’s Custom Events within its own advertising business, including to serve
 5 targeted ads, improve advertising-based machine learning models, and for research and development.
 6 *See* Ex. 86 at 20-25, 27-34; Ex. 38, Meta’s Resp. to Rog. No. 1 at 13 (Meta admitting Flo App event
 7 data was “used to improve, through machine learning, the accuracy of content delivery, including
 8 delivery of advertisements from advertisers besides Flo Health.”); Ex. 84 at 114:3-8 (same); Ex. 127
 9 (explaining event data with AD IDs is used for re-targeting and attribution, and that there are “many
 10 more ways” Meta uses this data “downstream[,]” including to update “user features” based on their
 11 “interest or intent,” and having “ML models” recommend other “relevant” ads to them); Ex. 85 at
 12 ‘161 (Meta made Flo data “available for [its] Core Data Science research and development team, or
 13 other engineers” to improve its other products like its “ads delivery systems” or to “identify potential
 14 opportunities to develop new products.”).

15 Google (like Meta) used Flo data to train machine learning models used for advertising and
 16 analytics. *See* Ex. 87 at ‘918 (Google used data collected from Flo to enhance its products, features,
 17 and services; “main value” Google gets from providing its SDKs is the “data sharing” and its ability
 18 to use the event data for its own purposes); Ex. 88 at ‘297 (Google explaining to Flo that its “machine
 19 learning model” uses “information to generate a prediction”); Ex. 89 at ‘258-59 (explaining app
 20 campaigns’ “success” depend on Google’s “proprietary machine learning technology,” which
 21 requires a “strong analytics tool that is collecting these data points and passing them to Google Ads”);
 22 Ex. 128 (explaining use of Google’s SDKs will lead to “REDACTED” in “revenue”).

23 Flurry too collected app event data for advertising and machine learning purposes, and
 24 provided its parent company, Yahoo, with a data feed containing the Custom Events for its own use,
 25 including to build individual marketing profiles. *See, e.g.,* Ex. 90 at ‘444 (explaining Yahoo and
 26 Flurry have “create[d] a data feed that contains all the events captured from . . . Flurry[’s] Analytics
 27 SDK.”); Ex. 91 at 68:24-69:4 (explaining this feed was “the source of the Flurry data that was made
 28 available to Yahoo”); *id.* at 57:16-58:2 (“Q: So was the purpose of collecting data or the value of

collecting data for Flurry to use it for advertising purposes?” . . . “[A]: . . . I would say, . . . yes.”); Ex. 129 at ‘877-78 (explaining this feed was used for creating “targeting segments,” “identity [i]mapping,” and “profile building”); Ex. 130 at ‘466 (explaining data from Flurry Analytics is used to make “unique user profiles” that include “300 diff. interest categories”); Ex. 131 at 150:20-24 (admitting Flurry used app data for machine learning).

Flo Breaches its Promises to Flo Users. Flo repeatedly promised Flo App Users that it would only share their personal information in accordance with its privacy policy. Flo never disclosed that it would share users’ actual health information and, in fact, repeatedly promised it would not do so. See Exs. 92-106 (Flo’s Privacy Policies throughout the Class Period). Flo doubled down on these misrepresentations. When asked by a Flo App user what “information” Flo shared with “other organizations,” Flo represented “[a]lmost all the information [i] shared is anonymous and aggregated” and that the only reason it shared any information was because “[t]he application will not be able to operate if we don’t do it.” Ex. 107 at ‘363. That was a lie, as the Flo App still operates today after it purportedly stopped sharing user data.

Defendants’ Continuous Misconduct. On February 22, 2019, the *Wall Street Journal* published an article “You Give Apps Sensitive Personal Information. Then They Tell Facebook.” The article discussed several apps, including Flo, sharing sensitive data with Facebook. The FTC subsequently served Flo with a Civil Investigative Demand on June 18, 2019, seeking information related to its “disclosure of Fertility Information” to third parties. Ex. 108. Undeterred, Flo contacted Google on June 19, 2019 to evaluate alternatives for transmitting health data that would avoid the “bad PR” associated with SDKs. Ex. 109; Ex. 110. Flo did the same with Meta, proposing to share data directly from its servers, concealing the practice and thus creating “less issues for journalists.” Ex. 111 at ‘171. Google was encouraging. Afraid of losing data from “the biggest app in the health category,” Google tried to “convince [Flo]” to ignore the “PR” risk and continue using its “Firebase SDK.” Ex. 109 at ‘395 (“bring on the PR – we’re ready”). Meta also sought to prevent Flo from removing its SDK, concerned it would lose [REDACTED] on ads. Ex. 112 at ‘721. After Flo informed Meta that Apple would ban its app if they did not “remove any third party SDKs” following the *WSJ*’s report, Meta discussed contacting the “Apple Partnerships team” to reverse that

1 decision. Ex. 113 at ‘236. The FTC finalized a settlement with Flo in June 2021. *In the Matter of Flo*
 2 *Health, Inc.*, FTC No. C-4747, Decision and Order (June 17, 2021). Flo agreed to obtain users’
 3 affirmative consent before sharing personal health information, and to notify affected Flo App users
 4 whose health information it disclosed to third parties. *Id.* at 4. Email notices alerting users that their
 5 data had been shared were sent beginning on or around June 30, 2021. Ex. 114 at ‘587.

6 **III. LEGAL STANDARD**

7 “Before it can certify a class, a district court must be satisfied, after rigorous analysis, that the
 8 prerequisites of both Rule 23(a) and 23(b)(3) have been satisfied.” *Olean Wholesale Grocery Coop.,*
 9 *Inc. v. Bumble Bee Foods LLC*, 31 F.4th 651, 664 (9th Cir. 2022) (internal quotation omitted). “Merits
 10 questions may be considered to the extent—but only to the extent—that they are relevant to
 11 determining whether the Rule 23 prerequisites for class certification are satisfied.” *Amgen Inc. v.*
 12 *Conn. Ret. Plans and Tr. Funds*, 568 U.S. 455, 466 (2013).

13 **IV. ARGUMENT**

14 **A. The Proposed Classes Meet Rule 23(a)’s Requirements.**

15 Numerosity. Rule 23(a)(1) is satisfied when the “class is so numerous the joinder of all
 16 members is impracticable.” Fed. R. Civ. P. 23(a)(1). Here, each of the Proposed Classes consists of
 17 millions of individuals.⁸ See Ex. 1; see also *In re Static Random Access Memory (SRAM) Antitrust*
 18 *Litig.*, 264 F.R.D. 603, 608 (N.D. Cal 2009) (numerosity satisfied even when “exact size” was
 19 unknown because “general knowledge and common sense indicate that [the class] is large”).

20 Commonality. Rule 23(a)(2) is satisfied when there are “questions of law or fact common to
 21 the class.” Fed. R. Civ. P. 23(a)(2). Even if there are “circumstances of each particular class member
 22 [that] vary,” so long as there are “common core of factual or legal issues with the rest of the class,
 23 commonality exists.” *Parra v. Bashas’, Inc.*, 536 F.3d 975, 978-79 (9th Cir. 2008). Only a single
 24 common question of law or fact is required. See *In re JUUL Labs, Inc., Mktg. Sales Pracs. & Prod.*
 25 *Liab. Litig.*, 609 F. Supp. 3d 942, 960 (N.D. Cal. 2022). Here, Plaintiffs’ and the Classes’ claims arise
 26 from the same core set of facts and give rise to multiple common questions of both law and fact

27
 28 ⁸ Despite having it, Flo has refused to provide the exact number of Flo App Users/California Flo App Users who completed the Flo onboarding survey and entered menstrual information in the Flo App.

1 regarding, among other things, the interception and use of Class members' health information without
2 consent. *See* Section IV(B) *infra*. Because common evidence relating to these common questions
3 "will resolve an issue that is central to the validity of each one of the claims in one stroke,"
4 commonality is satisfied. *Rodriguez v. Google LLC*, No. 20-CV-04688-RS, 2024 WL 38302, at *3
5 (N.D. Cal. Jan. 3, 2024) (citing *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011)).

6 Typicality. Rule 23(a)(3) evaluates "whether other members have the same or similar injury,
7 whether the action is based on conduct which is not unique to the named plaintiffs, and whether other
8 class members have been injured by the same course of conduct." *Wolin v. Jaguar Land Rover N.*
9 *Am., LLC*, 617 F.3d 1168, 1175 (9th Cir. 2010) (internal citation omitted). As described above, each
10 Plaintiff—and all Class/Subclass members—used the Flo App, completed the onboarding survey,
11 and, as a result, were injured when their sensitive health information was intercepted and used without
12 their consent. Plaintiffs are therefore typical of all Class/Subclass members because they suffered the
13 same injury as a result of the same course of conduct, by the same Defendants.

14 Adequacy. The adequacy requirement of Rule 23(a) demands that class representatives and
15 their counsel have no conflicts of interest with other class members and will vigorously prosecute the
16 litigation on behalf of the entire class. *See In re Yahoo Mail Litig.*, 308 F.R.D. 577, 595 (N.D. Cal.
17 2015) (citing *Staton v. Boeing Co.*, 327 F.3d 938, 957 (9th Cir. 2003)). Plaintiffs' declarations
18 establish that: (1) there are no conflicts of interest among the class representatives or any members of
19 the Class; and (2) Plaintiffs and their counsel have vigorously prosecuted this litigation and will
20 continue to do so.

21 **B. Common Questions of Law and Fact Predominate Over Individual Issues.**

22 Plaintiffs seeking to certify a Rule 23(b)(3) damages class must show that common questions
23 predominate over individual ones. *See Olean*, 31 F.4th at 664 ("Rule 23(b)(3) overlap[s] with" Rule
24 23(a)). "An individual question is one where members of a proposed class will need to present
25 evidence that varies from member to member, while a common question is one where the same
26 evidence will suffice for each member[.]" *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 453 (2016)
27 (internal quotations omitted). This requirement is satisfied where "the common, aggregation-
28 enabling[] issues in the case are more prevalent or important than the non-common, aggregation-

defeating, individual issues.” *Olean*, 31 F.4th at 664 (quoting *Tyson Foods*, 577 U.S. at 453). “When one or more of the central issues in the action are common to the class and can be said to predominate, the action may be considered proper under Rule 23(b)(3) even though other important matters will have to be tried separately[.]” *Id.* at 668 (quoting *Tyson Foods*, 577 U.S. at 453). A district court’s predominance inquiry begins with the elements of each of Plaintiffs’ claims. *See id.* at 665 (internal citation omitted); *Nitsch v. Dreamworks Animation SKG Inc.*, 315 F.R.D. 270, 288 (N.D. Cal. 2016) (same).

C. The Claims of the Classes Satisfy Predominance

1. California Law Applies to Each of the Classes’ Claims

California law applies to each of the Nationwide Damages Class’s claims. Flo’s Terms of Use uniformly provide that “[a]ny dispute arising . . . shall be governed by the laws of the State of [California] without regard to its conflict of laws provisions.” *See, e.g.*, Ex. 115 at ‘573; Ex. 116 at ‘584; Ex. 117 at ‘555. The application of California law is also appropriate against the Ad Defendants who, like Flo, are based in California such that (1) California law presumptively governs their conduct (*see Ward v. United Airlines, Inc.*, 9 Cal. 5th 732, 750 (2020) (“[C]ourts ordinarily interpret California statutes to apply to conduct occurring anywhere within California’s borders, absent evidence a more limited scope was intended.”)); and (2) the “application of California law here poses no constitutional concerns.” *In re Qualcomm Antitrust Litig.*, 292 F. Supp. 3d 948, 978 (N.D. Cal. 2017).

2. Claims Against Flo

Plaintiffs assert the following claims on behalf of the Nationwide Damages Class against Flo: (1) CMIA; (2) breach of contract (or implied contract); (3) intrusion upon seclusion; and (4) CDAFA.

a. CMIA

The CMIA prohibits a “provider of health care” from sharing “any individually identifiable information, in electronic or physical form, in position of or derived from a provider of health care . . . regarding a patient’s medical history, . . . physical condition, or treatment.” Cal. Civ. Code §§ 56.10; 56.05(i); 56.05(o). The term “provider of health care” under § 56.06(b) includes “[a]ny business that offers software or hardware to consumers, *including a mobile application* or other related device that is designed to maintain medical information in order to make the information

1 available to an individual . . .” (emphasis added). Information allegedly disclosed must be “viewed”
 2 by an “unauthorized party” to establish injury. *Vigil v. Muir Med. Grp. IPA, Inc.*, 84 Cal. App. 5th
 3 197, 213 (Cal. Ct. App. 2022).

4 These elements raise several common questions subject to common proof. *See In re Premera*
 5 *Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-MD-2633-SI, 2019 WL 3410382, at *20 (D.
 6 Or. July 29, 2019) (finding “common issues of law and fact predominate” in CMIA claim). Whether
 7 Flo is a “provider of health care” under Cal. Civ. Code § 56.05(i) is answered by the Flo App itself,
 8 which Flo claims allows individuals to take “full control of [their] health” by tracking their menstrual
 9 cycles, pregnancies, and other aspects of reproductive health. Ex. 4 at ‘090; Ex. 3 at ‘360-61; Ex. 118
 10 at ‘624 (explaining Flo provides “personalized predications” for “luteal and follicular phases,
 11 ovulation, periods, fertility and much more”); Ex. 119 at ‘557 (aim to “make Flo a ‘family doctor’”).
 12 Flo reinforced the health focus of its app by promoting its medical board, composed of dozens of
 13 health experts, who developed content for the app and advised on its features. Ex. 120 at ‘149; Ex.
 14 118 at ‘629 (Flo “review[s] [its] articles, courses, and tools with” its medical board, comprising “some
 15 of the world’s top health experts from leading European and North American medical schools”).

16 Likewise, data reflecting Class members’ use of the Flo app, along with the information
 17 transmitted to and received by Ad Defendants will provide common proof of whether Flo shared
 18 medical information in violation of Cal. Civ. Code § 56.05(i). For example, data⁹ associated with
 19 each Named Plaintiffs’ Flo account shows they input menstrual cycle information in the Flo App and
 20 therefore also completed the onboarding survey. *See* Section II, pp. 7-8. That Ad Defendants received
 21 the events associated with these actions are reflected in their interrogatory responses, documents, and
 22 further confirmed by Plaintiffs’ expert testing. *See* Section II, pp. 4-8.

23 Whether Flo’s disclosure of medical information to third parties without authorization was in
 24 violation of Cal. Civ. Code § 56.10 is also subject to common proof. None of the Privacy Policies
 25 incorporated into Flo’s Terms of Use ever disclosed that Flo would share health information. *See*

26
 27 ⁹ Flo maintains this data for all Class members. Using this data, Flo calculated aggregated statistics
 28 reflecting, for each month, the total number of U.S. users who “registered” for the Flo App and which
 percentage of users in the U.S. selected each of the respective goal options in the onboarding survey.
See Ex. 1. These aggregated statistics and the underlying data they are common evidence.

Section II, p. 11, above. Similarly, common evidence shows that the data was “viewed,” as Ad Defendants incorporated that data into their ad delivery systems, products, and services, or otherwise used it for their own commercial purposes. *See* Section II, pp. 8-10.

b. Breach of Contract

Breach of contract has four elements: (1) existence of a contract; (2) performance under the contract; (3) Defendants’ breach; and (4) damages. *Roley v. Google LLC*, Case No. 18-v-07537-BLF, 2020 WL 8675968, at *10 (N.D. Cal. July 20, 2020). Courts in this district routinely find common issues predominate and certify classes pursuing breach of contract claims where they turn on a common set of policies. *See, e.g., Kumandan v. Google, LLC*, No. 19-cv-04286-BLF, 2023 WL 8587625, at *12, *18 (N.D. Cal. Dec. 11, 2023) (certifying breach of contract class of purchasers alleging violation of privacy policies); *Dulberg v. Uber Techs., Inc.*, No. C 17-00850 WHA, 2018 WL 932761, at *4-5 (N.D. Cal. Feb. 16, 2018) (certifying breach of contract class and holding that “[i]nterpretation of that agreement will, of course, apply on a class-wide basis”).

Like these cases, Plaintiffs’ and Class members’ use of the Flo App were governed by a common set of Terms of Use and Privacy Policies throughout the Class Period. *See* Section II, p. 11. Those policies made a common set of promises to all Class members, including about what specific data Flo would not share with others. *See* Section II p. 11 above. This presents numerous common questions that can be established with common evidence. For instance, whether Flo made uniform representations to class members about information it would share with Ad Defendants is a common question that can be answered using the policies available during the Class Period. *See* Section II, p. 11. Similarly, whether Flo breached those promises can be answered by an analysis of the data in Flo’s possession as well as the data the ADs acknowledge they received. *See* Section II, pp. 4-8.¹⁰

c. Intrusion Upon Seclusion

Intrusion upon seclusion has two elements: “whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive.” *In re Facebook, Inc. Internet Tracking*, 956 F.3d 589, 601 (9th Cir. 2020) (internal quotations omitted). These elements are evaluated under an

¹⁰ To the extent the Court finds an express contract does not exist, Plaintiffs have pled a breach of an implied contract claim in the alternative and can prove that claim using the same common proof.

1 objective standard. *See Rodriguez*, 2024 WL 38302 at *4-5 (certifying intrusion upon seclusion class
 2 and stating “the question of whether a reasonable expectation of privacy exists is an objective one”);
 3 *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1076 (N.D. Cal. 2021) (explaining standard is
 4 “objective[.]”); *Opperman v. Path, Inc.*, No. 13-cv-0453-JST, 2016 WL 3844326, at *11 (N.D. Cal.
 5 July 15, 2016) (rejecting argument that “an individual inquiry will be required into the subjective
 6 expectations of each class member” and certifying class for intrusion upon seclusion claim).

7 Whether Plaintiffs have a reasonable expectation of privacy can be answered objectively with
 8 the same common proof as their contract claim—polices showing that Flo “set an expectation” health
 9 information would not be shared. *Facebook Tracking*, 956 F.3d at 602 (plaintiffs’ stated intrusion
 10 upon seclusion claim based on Facebook’s privacy policies); *Brown*, 525 F. Supp. 3d at 1066 (finding
 11 reasonable expectation of privacy where “statements suggest that a user’s activity in private browsing
 12 mode is not saved or linked to the user”); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 621, 631
 13 (N.D. Cal. 2021) (finding reasonable expectation of privacy where the privacy notice “makes specific
 14 representations that could suggest to a reasonable user that [defendant] would not engage in the
 15 alleged data collection”); *Rodriguez*, 2024 WL 38302, at *5 (holding whether plaintiffs had an
 16 “objective, reasonable expectation of privacy . . . is a question capable of resolution class-wide”).

17 Whether a reasonable person would find Flo’s conduct highly offensive is also subject to
 18 common proof. *See id.* (rejecting argument that deciding whether the intrusion was highly offensive
 19 “requires consideration of all the circumstances of intrusion” and explaining that “the central inquiry
 20 [is] whether a *reasonable person* would find the intrusion by Google highly offensive”) (internal
 21 citation omitted) (emphasis in original); *Facebook Tracking*, 956 F.3d at 606 (analyzing whether
 22 invasion is “highly offensive to a reasonable person,” with a “focus[] on the degree to which the
 23 intrusion is unacceptable as a matter of public policy”). The unauthorized disclosure of sensitive
 24 health information is uniformly recognized as a highly offensive violation of privacy. *Doe v. Regents*
 25 *of Univ. of California*, No. 23-CV-00598-WHO, 2023 WL 3316766, at *6 (N.D. Cal. May 8, 2023)
 26 (finding collection of health information highly offensive because “[p]ersonal medical information is
 27 understood to be among the most sensitive information that could be collected about a person”). Here,
 28 internal documents show that Flo, along with other Ad Defendants, not only recognized that Flo was

1 sharing health information but assisted Flo in using that data for advertising. *See* Section II, pp. 8-10.
 2 This is objectively highly offensive, as shown by this common evidence.

3 **d. CDAFA**

4 CDAFA requires proof that the Defendants: (a) “knowingly accesses and without permission
 5 takes, copies, or makes use of any data from a computer” (Cal. Penal Code § 502(c)(2)); or (b)
 6 “knowingly and without permission provides or assists in providing a means” of “accessing a
 7 computer, computer system, or computer network in violation of this section.” *See* Cal. Penal Code
 8 § 502(c)(6); *see also Ticketmaster L.L.C. v. Prestige Ent. W., Inc.*, 315 F. Supp. 3d 1147, 1176 (C.D.
 9 Cal. 2018) (finding a defendant violated subsection (c)(6) by providing means for others to “commit
 10 violations of . . . other subsections of the CDAFA”). Plaintiffs also must show they “suffer[ed]
 11 damage or loss by reason of a violation.” Cal. Penal Code § 502(e)(1).

12 Common evidence will prove each of these requirements. Documents as well as expert testing
 13 of the Flo App show that Flo provided the means and assistance for Ad Defendants to take and use
 14 sensitive health information from Nationwide Damages Class Members’ mobile devices. The same
 15 documents show Flo acted knowingly, as it intended to use the data collected through Ad Defendants’
 16 SDKs for multiple purposes. *See* Section II, pp. 8-10. That Flo’s conduct was “without permission” is
 17 established by Flo’s Privacy Policies, none of which disclose that Flo would share or permit others to
 18 access and use Nationwide Damages Class Members’ health data. *See Greenley v. Kochava, Inc.*, No.
 19 22-CV-01327-BAS-AHG, 2023 WL 4833466, at *13 (S.D. Cal. July 27, 2023) (finding the “without
 20 permission” requirement satisfied where plaintiff “did not ‘consent’ to Defendant’s data collection”).

21 Lastly, all Nationwide Damages Class Members suffered a “loss” that can be established
 22 through common proof. *See Rodriguez*, 2024 WL 38302 at *6 (finding that questions of whether
 23 plaintiffs’ data carried financial value and whether defendants profited from the data could be
 24 established “class-wide” and certifying CDAFA class). As Plaintiffs’ expert Prof. David Hoffman
 25 explained, the value of the health data Defendants misappropriated is confirmed by: (1) the existence
 26 of a market for this information, and (2) Defendants’ conduct in using the data for commercial
 27 purposes. *See* Ex. 121 at § III.D. Indeed, Flo was an active participant in this market – selling access
 28 to this Custom Event data. *Id.* at § III.E. Flo’s misappropriation of that valuable data is common harm

1 sufficient to support CDAFA claims. *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 964
 2 (N.D. Cal. 2014) (explaining for the CDAFA “any amount of damage or loss caused by the
 3 defendant’s CDAFA violation is enough to sustain the plaintiff’s claims”). CDAFA does not require
 4 Plaintiffs measure the precise loss for each class member to meet this requirement.

5 **3. Claims Against Ad Defendants**

6 **a. CDAFA**

7 Common evidence shows that the Ad Defendants violated CDAFA by knowingly intercepting
 8 and using data intercepted from Flo Nationwide Damages Class Members’ devices through their
 9 SDKs. *See CTI III, LLC v. Devine*, No. 2:21-CV-02184-JAM-DB, 2022 WL 1693508, at *4 (E.D.
 10 Cal. May 26, 2022) (explaining CDAFA “does not require *unauthorized* access . . . [but] merely
 11 requires *knowing* access”). Ad Defendants’ guides and marketing materials show that they knowingly
 12 “access” data from computer systems (i.e., mobile devices) through their SDKs. *See* Cal. Penal Code
 13 § 502(b)(1) (defining “access” as “to gain entry to, instruct, cause input to, cause output from, cause
 14 data processing with, or communication with . . . resources of a computer”). Indeed, Ad Defendants
 15 acknowledge that this is the purpose of incorporating their SDKs into a mobile application. *See* Ex. 5
 16 ¶53 (explaining purpose of SDKs is to access data from the device); Ex. 18 (explaining Meta SDKs
 17 access event data); Ex. 11 (same); Ex. 19 (same). As described in Section II, the Ad Defendants’
 18 interception and use of data from Class members’ devices through their SDKs provides common
 19 proof of their CDAFA claims.

20 **b. Aiding and Abetting Intrusion Upon Seclusion**

21 An adding and abetting claim requires showing the Ad Defendants: (1) knew Flo’s conduct
 22 constituted an invasion of privacy and gave substantial assistance or encouragement to Flo, or (2)
 23 gave substantial assistance to Flo in accomplishing an invasion of privacy, and that their own conduct,
 24 separately constituted an invasion of privacy. *See Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 985
 25 (N.D. Cal. 2015); *see also Opperman*, 2016 WL 3844326, at *3 (certifying class for aiding and
 26 abetting intrusion upon seclusion claim). Plaintiffs’ claim that the Ad Defendants aided and abetted
 27 Flo’s intrusion upon their seclusion will be supported by the same common evidence described above:
 28 (1) showing that Flo violated their privacy rights and (2) that Ad Defendants, in designing their SDKs

to intercept this data, and coordinating with Flo to facilitate the collection and use of this information, provided substantial assistance to Flo’s violation. *See* Section II.

D. The California Subclass

Plaintiffs seek certification of a California Subclass asserting the same claims as their Nationwide Damages Class (*i.e.*, CMIA, Breach of Contract, Intrusion Upon Seclusion, and CDAFA), against the same Defendants, and two additional California-specific claims. California residents can be identified in Flo’s data or through self-identifying individuals. *McCrary v. Elations Co., LLC*, No. EDCV 13-00242 JGB OP, 2014 WL 1779243, at *7 (C.D. Cal. Jan. 13, 2014) (finding class ascertainable where plaintiff “proposes that class members self-identify their inclusion [in the class] via affidavits” because “[t]he class definition is sufficiently definite so that it is administratively feasible to determine whether a particular person is a class member”).

1. Invasion of Privacy Under the California Constitution Against Flo

“Because of the similarity of the tests [for constitutional invasion of privacy and common law intrusion claims], courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive. *Facebook Tracking*, 956 F.3d at 601. Given that both claims consider the same elements, Plaintiffs can establish their California Constitution claim using the same evidence discussed in Section II.

2. Violation of CIPA Against the Ad Defendants

Common evidence will show the Ad Defendants violated both CIPA’s Section 631 and 632. Section 631 “prohibits any person from using electronic means to learn the contents or meaning of any communication without consent or in an unauthorized manner.” *Facebook Tracking*, 956 F.3d at 607 (internal quotations omitted). Attempts to intercept and use of intercepted communications are equally forbidden under § 631(a). *Greenley*, 2023 WL 4833466, at *16 (explaining that this section also punishes “persons who attempt to learn in an unauthorized manner the contents of communications passing over any wires, lines, and cables”). Section 632 prohibits unauthorized recording or eavesdropping on confidential communications. *See In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *22 (N.D. Cal. Sept. 26, 2013); *see also In re Meta Pixel Healthcare Litig.*, No. 22-cv-03580-WHO, 2022 WL 7869218, at *13 (N.D. Cal. Dec. 22, 2022)

(delineating between § 631’s “wiretapping provision” and § 632’s “recording provision”).

Plaintiffs’ CIPA claims present common questions answerable by common proof. Ad Defendants’ documents and interrogatories show that they intercepted (in violation of § 631) and recorded (in violation of § 632) the contents of Plaintiffs’ and Class members’ communications with Flo by capturing Custom Events reflecting health information they entered into the Flo app. *See* Section II, pp. 2-8. Common evidence also shows that each Ad Defendant used the health information it intercepted from Flo users. *See* Section II, pp. 8-11. Each Ad Defendant’s intent to capture such information is reflected in the design of the SDKs, whose very purpose is to collect and transmit data. *See* Section II, pp. 2-3. Meta and Google further demonstrated intent by their efforts to discourage or prevent Flo from removing their SDKs, and eagerness to explore alternative means of acquiring the same health information. *See* Section II, pp. 11-12. Finally, lack of authorization is also a common question that can be answered by Flo’s policies, which did not obtain consent to share health information and expressly stated that health information would not be shared with any third parties. *See* Section II, p. 11.

E. Common Issues Predominate Regarding the Relief Plaintiffs Seek

Plaintiffs pursuing damages under Rule 23(b)(3) must show the monetary relief they seek is “capable of measurement on a classwide basis,” in the sense that the whole class suffered damages traceable to the same injurious course of conduct.” *Just Film, Inc. v. Buono*, 847 F.3d 1108, 1120 (9th Cir. 2017) (quoting *Comcast Corp. v. Behrend*, 569 U.S. 27, 34-35 (2013)); *see also Owino v. CoreCivic, Inc.*, 60 F.4th 437, 447 (9th Cir. 2022) (same). These calculations “need not be exact,” *Brown v. Google, LLC*, No. 20-cv-3664-YGR, 2022 WL 17961497, at *5 (N.D. Cal. Dec. 12, 2022) (citing *Comcast*), and “damage calculations alone cannot defeat certification.” *Pulaski & Middleman*, 802 F.3d 979, 986 (9th Cir. 2015) (quoting *Yokoyama v. Midland Nat. Life Ins. Co.*, 594 F.3d 1087, 1094 (9th Cir. 2010)). The remedies that Plaintiffs seek for their claims are articulated below.

1. Statutory Damages

Plaintiffs seek statutory damages on behalf of the Classes in connection with their CMIA claims against Flo and CIPA claims against the Ad Defendants. The CMIA awards \$1,000 per violation. *See* CMIA § 56.36(b)(1). CIPA provides for a statutory minimum judgment of \$5,000 per

violation. Cal. Penal Code § 637.2(a); *Steven Ades & Hart Woolery v. Omni Hotels Mgmt. Corp.*, No. 2:13-CV-02468-CAS, 2014 WL 4627271, at *14 (C.D. Cal. Sept. 8, 2014) (explaining “CIPA [] provides for statutory damages upon proof of a privacy violation, without evidence of actual damages” and that “issues of excessive damages are better addressed at a later stage of the litigation”).

For each of these claims, damages can be calculated formulaically and on a classwide basis by multiplying the number of violations proven by the amount awarded by the relevant statute. *Kellman v. Spokeo, Inc.*, No. 21-CV-08976-WHO, 2024 WL 2788418, at *11 (N.D. Cal. May 29, 2024) (“Statutory damages are calculated as prescribed by the statutes. What the statute provides is a common question of law, so common questions predominate for the damages analysis [].”); *Coulter v. Bank of Am.*, 28 Cal. App. 4th 923, 925 (1994) (affirming trial court’s award of the “total of \$132,000 in damages [under CIPA], \$3,000 for each of 44 specific violations”); *Francies v. Kapla*, 127 Cal. App. 4th 1381, 1385 (Cal. Ct. App. 2005) (affirming trial court’s award of CMIA statutory damages). Here, the number of violations can be established based on Defendants’ records, which reflect the number of times the Ad Defendants received the Custom Events in Figure 1. *See, e.g.*, Ex. 27 (number of times Meta received events in Figure 1); Ex. 24 (same for Google).

2. Punitive Damages

Under California law, punitive damages are available when a defendant acts with oppression, fraud, or malice. *See* Cal. Civ. Code § 3294. Courts have permitted punitive damages where defendants have committed an invasion of privacy. *Jackson v. First Nat’l Bank of Omaha*, No. CV 20-1295 DSF (JCX), 2022 WL 423440, at *9 (C.D. Cal. Jan. 18, 2022) (“California courts and district courts in the Ninth Circuit have recognized punitive damages may be appropriate for common law invasion of privacy claims.”); *Varnado v. Midland Funding LLC*, 43 F. Supp. 3d 985, 994 (N.D. Cal. 2014) (holding invasion of privacy can support punitive damages).

This presents common questions related to Defendants’ conduct that courts recognize are amenable to certification. *Ellis v. Costco Corp.*, 285 F.R.D. 492, 542-44 (N.D. Cal. 2012) (certifying Rule 23(b)(3) class including claim for punitive damages, explaining “the purpose of punitive damages is not to compensate the victim, but to punish and deter the defendant, . . . the focus of a punitive damages claim is not on facts unique to each class member, but on the defendant’s conduct

toward the class as a whole.”); *Opperman*, 2016 WL 3844326, at *16 (certifying 23(b)(3) class explaining “punitive damages . . . was best decided on a classwide basis”). This is true here, where the same evidence described above will prove Defendants acted with the requisite intent.

3. Nominal Damages

Plaintiffs seek nominal damages for the Classes in connection with their intrusion claims. *Opperman*, 2016 WL 3844326, at *16 (certifying invasion of privacy class for nominal damages); *Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 919 (S.D. Cal. 2020) (explaining the CMIA “provides for nominal damages” without showing “actual damages”); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp. 3d 1284, 1299 (S.D. Cal. 2020) (same).

Nominal damages are awarded for “the infraction of a legal right, where the extent of loss is not shown, or where the right is one not dependent upon loss or damage.” *Opperman v. Path, Inc.*, 2016 WL 3844326, at *16. An award of nominal damages does not require individualized inquiries because nominal damages are not “intended to compensate a plaintiff for injuries.” *Id.* at *16 (explaining “it is precisely ‘where the amount of damages is uncertain’ that nominal damages may . . . be awarded.”). Given this, “several district courts in the Ninth Circuit have certified classes involving claims for nominal damages.” *Id.* (collecting cases).

4. Disgorgement

It is a foundational principle of California law and federal equitable principles that a defendant shall not benefit from their own wrongdoing. *See Liu v. SEC*, 140 S.Ct. 1936, 1942 (2020) (“[e]quity courts have routinely deprived wrongdoers of their net profits from unlawful activity”); *Facebook Tracking*, 956 F.3d at 600 (“California law requires disgorgement of unjustly earned profits regardless of [plaintiffs’ damages].”) (emphasis added); *Meister v. Mensinger*, 230 Cal. App. 4th 381, 398 (Cal. Ct. App. 2014) (“‘[T]he public policy of this state does not permit one to “take advantage of his own wrong”’ regardless of whether the other party suffers actual damage.”). Documents showing the amount of money Flo: (1) paid to Meta and Google for advertising, and (2) profited from selling subscriptions to the Flo app while disclosing data in violation of its policies, provide common evidence of profits that should be disgorged. *See* Section II, p. 11.

F. A Class Action Is the Superior Method of Adjudicating This Dispute

Rule 23(b)(3)’s superiority requirement asks “whether the ends of justice and efficiency are served by certification.” *DZ Reserve v. Meta Platforms, Inc.*, No. 3:18-cv-04978-JD, 2022 WL 912890, at *9 (N.D. Cal. Mar. 29, 2022). Courts must consider the following factors to determine superiority: (1) the interest of each class member in controlling the prosecution or defense of separate actions; (2) the extent and nature of any litigation concerning the controversy already commenced; (3) the desirability of concentrating the litigation in the particular forum; and (4) the difficulties likely to be encountered in the management of a class action. Fed. R. Civ. P. 23(b)(3)(A)-(D).

Considering the first factor, courts regularly find superiority where the “risks, small recovery, and relatively high costs of litigation make it unlikely that plaintiffs would individually pursue their claims.” *Just Film, Inc.*, 847 F.3d at 1123 (internal citation omitted); *see also DZ Reserve*, 2022 WL 912890 at *9 (“[I]t is not likely for class members to recover large amounts individually if they prevailed. No reasonable person is likely to pursue these claims on his or her own”). Here, Class members’ individual damages would likely pale in comparison to the cost of litigation. The remaining factors also weigh in favor of certification: there are no other cases, each Defendant is based in this district, and a class action would be sufficiently manageable given the “variety of procedural tools courts can use to manage the administrative burdens of class litigation” and the objective criteria defining the Classes. *Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1131 (9th Cir. 2017).

G. The Proposed Injunction Class Meets Rule 23(b)(2)’s Requirements

Plaintiffs also seek to certify a nationwide class and a California subclass under Rule 23(b)(2) for injunctive relief in connection with their CIPA, CDAFA, and intrusion upon seclusion claims. Membership in the California subclass can be determined using Flo’s data or affidavits as described in Section II, p. 2. Unlike a damages claim, a Rule 23(b)(2) class does not require a showing of predominance or superiority. *In re Yahoo Mail*, 308 F.R.D. at 598. Rather, the class may be certified so long as class members “complain of a pattern or practice that is generally applicable to the class as a whole.” *DZ Reserve*, 2022 WL 912890, at *10.

Plaintiffs seek injunctive relief to stop Defendants’ ongoing exploitation of health information collected from Class members through the Ad Defendants’ SDKs. Each Ad Defendant received and

1 used health information via the Custom Events during the Class Period. *See* Section II, pp. 3-10.
 2 There is no evidence that this data has been removed from Ad Defendants' systems, or that their use
 3 of it (or data derived from it) has stopped. The Ad Defendants should each be required to destroy any
 4 Custom Event data received from Flo and immediately stop its use for all purposes, including as part
 5 of algorithms, systems, and processes that have incorporated that data.

6 Plaintiffs also seek an injunction that would require Flo to obtain separate, handwritten
 7 authorization to disclose Class members' medical information, as required by § 56.11 of CMIA that:
 8 (1) states the specific limitations and uses on the types of medical information disclosed (2) provides
 9 a specific date when Flo is no longer authorized to disclose the information, and (3) advises the person
 10 of their right to receive a copy of the notification. Flo should also be required to delete all data relating
 11 to or derived from Plaintiffs' sensitive health information, including any custom audiences for
 12 advertising created using this information. Finally, Flo should be ordered to undergo routine, yearly
 13 audits to ensure this injunctive relief has been (and remains) implemented. This is necessary given
 14 evidence that Flo sought to transmit health data through other means to circumvent detection after
 15 removing the Ad Defendants' SDKs from its App. Because the relief sought is applicable to the
 16 Injunctive Relief Class and Subclass as a whole, certification pursuant to Rule 23(b)(2) is proper.

17 **a. The Court Should Appoint Class Counsel.**

18 As demonstrated by Counsel's work thus far in this case, Interim Class Counsel possess the
 19 necessary knowledge, experience, and resources to prosecute this matter fairly and effectively. *See*
 20 Fed. R. Civ. P. 23(g)(4); Order re Co-Lead Counsel, ECF No. 80 at 1.

21 **V. CONCLUSION**

22 For the foregoing reasons, Plaintiffs' Motion should be granted in its entirety.

23
 24
 25 Dated: August 29, 2024

/s/ Carol C. Villegas

Carol C. Villegas (*pro hac vice*)

Michael P. Canty (*pro hac vice*)

Jake Bissell-Linsk (*pro hac vice*)

David Saldamando (*pro hac vice*)

Danielle Izzo (*pro hac vice*)

Gloria Medina (*pro hac vice*)

LABATON KELLER SUCHAROW LLP

140 Broadway
New York, NY 10005
Tel: (212) 907-0700
Fax: (212) 818-0477
cvillegas@labaton.com
mcanty@labaton.com
jbissell-linsk@labaton.com
dsaldamando@labaton.com
dizzo@labaton.com
gmedina@labaton.com

*Interim Co-Lead Counsel
for Plaintiffs and the Proposed Class*

Christian Levis (*pro hac vice*)
Amanda Fiorilla (*pro hac vice*)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

*Interim Co-Lead Counsel
for Plaintiffs and the Proposed Class*

Diana J. Zinser (*pro hac vice*)
Jeffrey L. Kodroff (*pro hac vice*)
Icee N. Etheridge (*pro hac vice*)
Cary Zhang (*pro hac vice*)
SPECTOR ROSEMAN & KODROFF, P.C.
2001 Market Street, Suite 3420
Philadelphia, PA 19103
Tel: (215) 496-0300
Fax: (215) 496-6611
dzinser@srkattorneys.com
jkodroff@srkattorneys.com
ietheridge@srkattorneys.com
czhang@srkattorneys.com

*Interim Co-Lead Counsel
for Plaintiffs and the Proposed Class*

Ronald A. Marron (CA Bar 175650)
Alexis M. Wood (CA Bar 270200)
Kas L. Gallucci (CA Bar 288709)
LAW OFFICES OF RONALD A. MARRON
651 Arroyo Drive
San Diego, CA 92103
Tel: (619) 696-9006

1 Fax: (619) 564-6665
2 ron@consumersadvocates.com
3 alexis@consumersadvocates.com
4 kas@consumersadvocates.com

5 *Counsel for Plaintiffs Jennifer Chen and Tesha*
6 *Gamino*

7 Kent Morgan Williams (*pro hac vice*)
8 **WILLIAMS LAW FIRM**
9 1632 Homestead Trail
10 Long Lake, MN 55356
11 Tel: (612) 940-4452
12 williamslawmn@gmail.com

13 William D. Harris, II (*pro hac vice*)
14 **HARRIS LEGAL ADVISORS LLC**
15 3136 Kingsdale Center, Suite 246
16 Columbus, OH 43221
17 Tel: (614) 504-3350
18 Fax: (614) 340-1940
19 will@harrislegaladvisors.com

20 *Counsel for Plaintiffs Leah Ridgway and Autumn*
21 *Meigs*